THE PI MU EPSILON 100TH ANNIVERSARY PROBLEMS: PART IV

STEVEN J. MILLER*

As 2014 marks the 100th anniversary of Pi Mu Epsilon, I thought it would be fun to celebrate with 100 problems related to important mathematics milestones of the past century. The problems and notes below are meant to provide a brief tour through some of the most exciting and influential moments in recent mathematics. As editor I have been fortunate to have so many people contribute (especially James Andrews and Avery Carr, who assisted greatly in Parts I and II); for each year a contributor has written a description of the event and proposed a problem for the reader's enjoyment. No list can be complete, and of course there are far too many items to celebrate. This list must painfully miss many people's favorites.

As the goal is to introduce students to some of the history of mathematics, accessibility counted far more than importance in breaking ties, and thus the list below is populated with many problems that are more recreational. Many others are well known and extensively studied in the literature; however, as the goal is to introduce people to what can be done in and with mathematics, I've decided to include many of these as exercises since attacking them is a great way to learn. We have tried to include some background text before each problem framing it, and references for further reading. This has led to a very long document, so for space issues we split it into four parts (based on the congruence of the year modulo 4). That said: Enjoy!

1916

Ostrowski's theorem

In algebra there is a generalized notion of absolute value that defines an absolute value as a function in a field that maps elements of the field to the positive real numbers. Any absolute value must satisfy the following four conditions.

1. $\|x\| \geq 0$.
2. $\|x\| = 0$ if and only if $x = 0$
3. $\|xy\| = \|x\|\|y\|$.
4. $\|x + y\| \leq \|x\| + \|y\|$.

Josef Kurschak was the first to lay out these axioms, doing so in 1912, although Kurt Hensel had started related research earlier, including introducing p-adic numbers in 1897.

The immediate example which should come to mind is the traditional absolute value, which is given by

$$\|x\| := \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0. \end{cases}$$

Another common example is the trivial absolute value,

$$\|x\|_0 := \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

For our discussion of Ostrowski's Theorem there is one more important type of absolute value, the p-adic absolute value. Given a nonzero rational number x and a

*Williams College, Editor

prime p, x can be written uniquely in the form $x = p^n a/b$ with n, a and b integers and a, b and p pairwise coprime. The p-adic absolute value is then defined on the rational numbers to be

$$\|x\|_p := \begin{cases} 0 & \text{if } x = 0 \\ p^{-n} & \text{if } x \neq 0 \text{ and } x = p^n a/b \text{ as above.} \end{cases}$$

Two absolute values, $\|\cdot\|_1$ and $\|\cdot\|_2$, are equivalent if $\|x\|_1 = \|x\|_2^c$ for some c for all x in the domain. Ostrowski's Theorem states that any absolute value on the rational numbers must be equivalent to the trivial absolute value, the standard absolute value or a p-adic absolute value.

Proven in 1916 by Alexander Ostrowski, one use has been used to justify the real numbers as the most natural extension of the rational numbers (just as the rational numbers extend the integers). The standard absolute value can be viewed as a map between the rationals and the positive real numbers. The p-adic absolute value, on the other hand, maps the rationals to the p-adic numbers. Since the standard absolute value has the additional property of being Archimedean, that is for an non-zero x, there exists an N such that for all $n > N$ the absolute value of the sum of n x's is greater than 1. Since this is a desirable property for a practical number system that the p-adic's do not satisfy, the only remaining extension of the rationals is the real numbers.

Centennial Problem 1916. *Proposed by David Burt and Steven J. Miller, Williams College.*

For the p-adic norm to be meaningful, it is important that each number x can be written uniquely for a given choice of prime p as $p^n a/b$ with n, a and b all integers and a and b coprime. Prove this. What does $\log_p(\|x\|_p)$ measure? Consider a number field such as $\mathbb{Q}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Q}\}$. Notice unique factorization is lost here, as $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ and no factor divides any other. Are there notions of absolute values here, and if so what are they?

REFERENCES

[1] A. Ostrowski, "Über einige Lösungen der Funktionalgleichung $\phi(x)\phi(y) = \phi(xy)$", Acta Mathematica (2nd ed.) **41** (1916), no. 1, 271–284.
[2] D. Armstrong, "What is a ADE?", http://www.math.miami.edu/~armstrong/ADE.html (updated July 2013).
[3] F. Oggier, "Introduction to Algebraic Number Theory", December 2013, http://www1.spms.ntu.edu.sg/~frederique/ANT10.pdf.
[4] WIKIPEDIA, "Absolute Value (algebra)", http://en.wikipedia.org/wiki/Absolute_value_(algebra).
[5] WIKIPEDIA, "Ostrowski's Theorem", http://en.wikipedia.org/wiki/Ostrowski's_theorem.

1920

Waring's Problem

Hardy and Littlewood wrote a series of influential papers in additive number theory. Before their work, certain problems on primes were considered by many to be unaccessible; after all, the key properties of primes involve multiplication and factorization, not addition. Their work, however, showed that one could attack additive problems involving primes. The first in this series was published in 1920, *Some problems of 'Partitio numerorum'; I: A new solution of Waring's problem.* Waring's problem states that for any k there is a $s = s(k)$ such that every positive integer is a sum of at most s perfect k-powers. While Lagrange proved that four squares suffice,

the general case was not shown to be possible until the work of David Hilbert over a hundred years later; in fact, for many values of k we still do not know the smallest value of s which can be used.

Hilbert's proof in 1909 is an existence proof, and as originally states does not provide bounds on how many k-powers are needed. This was remedied by Hardy and Littlewood in 1920 in their masterful paper, where they further develop the Circle Method which Hardy and Ramanujan had introduced in 1916-1917 in analyzing the partition function. Hardy and Littlewood obtained explicit bounds, which many authors have subsequently lowered. The Circle Method converts these problems to a delicate analysis of exponential sums; note

$$\int_0^1 \left(\sum_{n=0}^{N} e^{2\pi i n^k x}\right)^s e^{-2\pi i N x} dx$$

is the number of ways of writing N as a sum of s perfect k-powers. We break the region of integration into two parts, a collection of very small (where small depends on k, s and N) segments where the integrand has a large absolute value, and the complementary region where the exponential sum has a lot of cancellation. The larger s is, the less cancellation we need. Hardy and Littlewood showed we may take $s(k) = 2^k + 1$; the current best bounds are on the order of $k \log k$.

Centennial Problem 1920. *Proposed by Steven J. Miller, Williams College.*

Often a related problem is significantly easier to attack than the original. This is the case for the well-studied *Easier Waring's Problem*, which asks given a positive integer k is there a $\nu(k)$ such that every integer can be written as a sum and difference of at most $\nu(k)$ perfect k-powers; in other words, given any N there are $\epsilon_1, \dots, \epsilon_{\nu(k)} \in \{-1, 0, 1\}$ and positive integers $n_1, \dots, n_{\nu(k)}$ such that $N = \epsilon_1 n_1^k + \cdots \epsilon_{\nu(k)} n_{\nu(k)}$. Prove the Easier Waring's Problem. *Hint:* $\nu(k) \le 2^{k-1} + \frac{1}{2}k!$.

REFERENCES

[1] G. H. Hardy and J. E. Littlewood, "Some problems of 'Partitio numerorum'; I: A new solution of Waring's problem", Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse (1920), 33–54. https://eudml.org/doc/59073.

[2] G. H. Hardy and J. E. Littlewood, "Some problems of 'Partitio Numerorum'; IV. The singular series in Waring's Problem and the value of the number $G(k)$", Mathematische Zeitschrift **12** (1922), no. 1, 161–188.

[3] G. H. Hardy and J. E. Littlewood, "Some problems of 'Partitio Numerorum'; VI. Further researches in Waring's problem", Mathematische Zeitschrift **23** (1925), no. 1, 1–37.

[4] G. H. Hardy and S. Ramanujan, "Asymptotic formulae in combinatorial analysis", Proc. London Math. Soc. **17** (1918), 75–115.

[5] M. Nathanson, "Additive Number Theory: The Classical Bases", Graduate Texts in Mathematics, Springer-Verlag, New York, 1996.

[6] P. Pollack, "On Hilbert's solution of Waring's Problem", Central European Journal of Mathematics **9** (2012), no. 2, 294–301. http://www.math.uga.edu/~pollack/riegerdress.pdf.

1924

The Banach-Tarski Paradox

The Banach-Tarski paradox: There exists a decomposition of a solid ball into a finite number of pieces that can be put back together in a different way to yield two identical copies of the original ball. In more everyday language, you can cut up an orange and reassemble it into two full-sized oranges. This is clearly not possible in practice - hence "paradox". The problem is, whereas real oranges are made of atoms and cut with a knife, mathematical oranges are made of infinitely many points and

can be cut into extremely complicated sets. You could imagine choosing, one by one, which piece each point should belong to, with no regard for nearby points. The actual construction is more subtle, but does involve making (uncountably) infinitely many arbitrary choices. Such constructions are permitted by the Axiom of Choice, which was introduced by Zermelo in 1904, and can be compactly phrased as "the product of a collection of non-empty sets is non-empty". Some see the Banach-Tarski paradox as a reason to reject the Axiom of Choice. The decomposition violates common sense, and the pieces can never be concretely defined, since you would never finish making choices. Therefore it seems reasonable to say that it does not exist, and in general, mathematical constructions should only be allowed to involve finitely many choices. However the Axiom of Choice is so useful that most mathematicians are willing to accept the existence of sets that have strange properties and cannot be fully described.

Perhaps the most fruitful legacy of the Banach-Tarski paradox is in group theory. Banach and Tarski's proof starts not with the ball, but with the group SO(3) of rigid rotations of the ball. They show that SO(3) contains disjoint subsets A, B, C, D and elements g, h such that both $A \cup gB$ and $C \cup hD$ are equal to SO(3). This led the mathematician John von Neumann to define amenable groups, which do not allow this or any similar "paradoxical decomposition". More precisely, a discrete group is *amenable* if and only if it has a finitely additive left-invariant probability measure. Such a measure gives a reasonable notion of "volume", which is exactly the concept that the Banach-Tarski paradox seams to violate.

Centennial Problem 1924. *Proposed by Stephen Bigelow, University of California, Santa Barbara.*

Is the Thompson group amenable? The Thompson group F was introduced by Thompson in 1965, and has unusual properties that make it a good source of counterexamples. It can be defined as the group of piecewise linear bijections from the unit interval to itself for which all non-differentiable points are dyadic rationals, and all slopes are powers of two. The question of its amenability is controversial. A preprint by Shavgulidze claims to show it is amenable, and one by Akhmedov claims to show it is not. The consensus seems to be that both preprints contain serious gaps, and the correct answer is not clear.

REFERENCES

[1] S. Banach and A. Tarski, "Sur la décomposition des ensembles de points en parties respectivement congruentes", Fundamenta Mathematicae **6** (1924), 244–277. http://matwbn.icm.edu.pl/ksiazki/fm/fm6/fm6127.pdf

1928

Random Matrix Theory

The name says it all: Random Matrix Theory is, as expected, the study of properties of randomly chosen matrices. What is not immediately apparent is why it should so beautifully model such diverse phenomena as energy levels of nuclear physics, the zeros of the Riemann zeta function (which encode information about the primes), and stopping times of bus routes in Mexican cities, to name just a few! While the subject began with Wishart's 1928 statistics paper in Biometrika in [1], for many people the exciting dates come later, in the 1950s, 1970s and 1990s.

In the 1950s Wigner [11, 12, 13, 14, 15] had the great insight that systems of random matrices could accurately predict properties of heavy nuclei. In any classical mechanics course one quickly learns how to solve in closed form a universe consisting of just one or two point masses; however, once we have three bodies in general configu-

ration then chaos sets in, and typically there is no longer a closed form of the solution. Imagine, then, how much more daunting the task is with heavy nuclei. There we have hundreds of protons and neutrons interacting under far more complicated forces than gravity. Quantum mechanically, we can represent this as $H\Psi_n = E_n\Psi_n$, where H is the Hamiltonian of the system, Ψ_n are the energy eigenstates with eigenvalues E_n. While this reduces quantum mechanics to linear algebra, it's linear algebra with a twist: the matrices are infinite by infinite, and we don't know any entries! Needless to say, this is well beyond the techniques learned in undergraduate classes on how to find eigenvalues.

Wigner's idea, which was rewarded with a Nobel prize, was that the complicated interaction actually *helps* us, if we change our perspective slightly. Rather than trying to find the eigenvalues of the operator associated to our physical system, Wigner looked at a bunch of random operators, diagonalized each of these, weighted the observed eigenvalue spectra by the probability of choosing that matrix, and then averaged over a family of matrices. The hope, which has been born out time and time again in experiments and theories, is that a 'typical' system is close to system average; a good way to view this universality is to see it as a central limit type theorem. Wigner's work was expanded by Dyson [2, 3] (who we'll meet again in a moment) and many others. These researchers mostly considered matrices where the independent entries were chosen from a fixed distribution (for example, physical grounds force many Hamiltonians to be real symmetric, which results in the independent entries being the main diagonal and the upper triangle part of the matrix).

Fast forward to the 1970s. The Riemann zeta function $\zeta(s)$ is defined, for real part of s greater than 1, by

$$\zeta(s) \ := \ \sum_{n=1}^{\infty} \frac{1}{n^s} \ = \ \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1},$$

and can be meromorphically continued to the entire complex plane with a simple pole of residue 1 at $s = 1$. The product expansion above follows from the Fundamental Theorem of Arithmetic (every positive integer can be written uniquely as a product of primes in non-decreasing order) and the geometric series formula. This product illustrates why the zeta function plays such a central role in modern number theory, as it connects the prime numbers (which are the building blocks of the integers, and objects we clearly wish to understand well) to the positive integers (which are very well understood!). Using complex analysis, one can show that the zeros of the completed zeta function are intimately connected to many properties of the primes. Montgomery was working on the pair correlation problem [9], trying to understand the distribution of differences of pairs of $\zeta(s)$. While visiting the Institute for Advanced Study at Princeton, he relayed what he had found to Dyson, who remarked that the same behavior is seen in the eigenvalues of certain ensembles of matrices! Additional support was later provided by the numerical investigations of Odlyzko on the zeros of $\zeta(s)$ (see [10] and Problem 1987).

From that moment, number theory, random matrix theory and physics had a lot to say to each other. The subjects continued to drive each other. New questions emerged in the 1990s with the work of Katz-Sarnak [6], expanding the universe of matrix families relevant to number theory. For more information on random matrix theory and its connection to number theory, see the books [7, 8] and the survey articles [1, 14, 15]; see also the entry from 1960 for an entertaining look at Wigner's views on the role of mathematics in physics.

Centennial Problem 1928. *Proposed by Steven J. Miller, Williams College.*

Let f be a nice probability distribution with mean 0, variance 1 and finite higher moments. For example, maybe f is the standard normal so $f(x) = e^{-x^2/2}/\sqrt{2\pi}$, or maybe f is the uniform distribution on $[-\sqrt[3]{3/2}, \sqrt[3]{3/2}]$. Consider the family of real symmetric matrices

$$\left\{ \begin{pmatrix} a_{11} & a_{11} \\ a_{21} & a_{22} \end{pmatrix} : a_{11}, a_{12}, a_{22} \text{ i.i.d.r.v. with density } f \right\};$$

this means that these three entries are chosen independently of each other, and the probability one of them is in the interval $[\alpha, \beta]$ is $\int_\alpha^\beta f(x)dx$. Calculate the probability that a randomly chosen matrix has its largest eigenvalue in the interval $[A, B]$. What about its smallest eigenvalue? What about the difference between its eigenvalues? *Hint: your old friend the quadratic formula can be helpful here, although if you try to do 3×3 or 4×4 matrices this approach becomes harder, and no such closed form expressions for the roots are available for $n \times n$ matrices once $n \geq 5$!*

REFERENCES

[1] J. B. Conrey, "L-Functions and random matrices". Pages 331–352 in *Mathematics unlimited — 2001 and Beyond*, Springer-Verlag, Berlin, 2001. http://arxiv.org/pdf/math/0005300.pdf?origin=publication_detail.

[2] F. Dyson, "Statistical theory of the energy levels of complex systems: I, II, III", J. Mathematical Phys. **3** (1962)140–156, 157–165, 166–175.

[3] F. Dyson, "The threefold way. Algebraic structure of symmetry groups and ensembles in quantum mechanics", J. Mathematical Phys., **3** (1962) 1199–1215.

[4] F. W. K. Firk and S. J. Miller, "Nuclei, Primes and the Random Matrix Connection", Symmetry **1** (2009), 64–105; doi:10.3390/sym1010064. http://arxiv.org/pdf/0909.4914.pdf.

[5] B. Hayes, "The spectrum of Riemannium", American Scientist **91** (2003), no. 4, 296–300. http://www.americanscientist.org/issues/pub/the-spectrum-of-riemannium.

[6] N. Katz and P. Sarnak, "Zeros of zeta functions and symmetries", Bull. AMS **36** (1999), 1–26.

[7] M. Mehta, "Random Matrices", 2nd edition, Academic Press, Boston, 1991.

[8] S. J. Miller and R. Takloo-Bighash, "An Invitation to Modern Number Theory", Princeton University Press, Princeton, NJ, 2006, 503 pages.

[9] H. Montgomery, "The pair correlation of zeros of the zeta function". Pages 181–193 in *Analytic Number Theory*, Proceedings of Symposia in Pure Mathematics, vol. 24, AMS, Providence, RI, 1973.

[10] A. Odlyzko, "On the distribution of spacings between zeros of the zeta function", Math. Comp. **48** (1987), no. 177, 273–308.

[11] E. Wigner, "On the statistical distribution of the widths and spacings of nuclear resonance levels", Proc. Cambridge Philo. Soc. **47** (1951), 790–798. http://journals.cambridge.org/abstract_S0305004100027237.

[12] E. Wigner, "Characteristic vectors of bordered matrices with infinite dimensions", Ann. of Math. **2** (1955), no. 62, 548–564.

[13] E. Wigner, "Statistical Properties of real symmetric matrices", Pages 174–184 in *Canadian Mathematical Congress Proceedings*, University of Toronto Press, Toronto, 1957.

[14] E. Wigner, "Characteristic vectors of bordered matrices with infinite dimensions. II", Ann. of Math. Ser. 2 **65** (1957), 203–207.

[15] E. Wigner, "On the distribution of the roots of certain symmetric matrices", Ann. of Math. Ser. 2 **67** (1958), 325–327.

[16] J. Wishart, "The generalized product moment distribution in samples from a normal multivariate population", Biometrika **20 A** (1928), 32–52.

1932

The $3x + 1$ Problem

The $3x + 1$ problem is a notorious unsolved problem. In one form it concerns iteration of the map defined by $T(2n) = n$ and $T(2n + 1) = 3n + 2$. The $3x + 1$ *Conjecture* asserts that iteration of this function starting from any positive integer

eventually reaches 1. That is, $T^{\circ k}(n) = 1$ for some $k \geq 1$, where $T^{\circ 2}(n) = T(T(n))$ denotes iterating the function twice. This problem is credited to Lothar Collatz, who certainly came up with similar problems in the 1930's. There are many great quotes about this. One describes it as a Soviet conspiracy to slow down American, as so many people tried working on it after hearing it, tempted by its simplicity to state. Another, due to Erdös, says that mathematics is not yet ready for problems such as this!

Centennial Problem 1932. *Proposed by Jeffrey Lagarias, University of Michigan.*

WARNING: This is an incredibly difficult problem: *Don't blame us if you try to solve it!* Here we consider *Collatz's original function*, which is the map on the integers defined by $g(3n) = 2n$, $g(3n+1) = 4n+1$ and $g(3n+2) = 4n+3$, which Collatz wrote down on July 1, 1932. This map is a permutation, and its inverse permutation $f(n) = g^{-1}(n)$ is given by $f(2n) = 3n$, $f(4n+1) = 3n+1$ and $f(4n+3) = 3n+2$. It is easily seen that $g(\cdot)$ maps the positive integers onto the positive integers, so it defines a permutation of the positive integers too. One finds that $g(1) = 1$ is a fixed point, $g(2) = 3, g(3) = 2$ is an periodic orbit of period 2, $g(4) = 5, g(5) = 7, g(7) = 9, g(9) = 6, g(6) = 4$ is a periodic orbit of period 5. What happens for $n = 8$? We arrive at the original Collatz problem: *Is the forward orbit of $n = 8$ under $g(\cdot)$ infinite? That is, prove that the orbit of 8 is not a periodic orbit.*

This problem has been proposed independently several times, for example in 1963 by Klamkin, with comments on it by Shanks and Atkin. It has been checked that the orbit of 8 includes numbers larger than 10^{400}. This could be extended by computer. **WARNING.** *This problem is unsolved, and could be as hopeless as the $3x+1$ problem.*

Here is a weaker problem, hence more approachable, which however also seems extraordinarily difficult.

1932 Subproblem 1. *Prove or disprove the assertion that the (full forward and backward) orbit of 8 has density 0. That is, if we define the set $S_x := \{1 \leq n \leq x :$ some iterate $g^{(k)}(8) = n$ or some iterate $g^{(k)}(n) = 8\}$ then the assertion states that $\lim_{x\to\infty} \frac{1}{x}\#(S_x) = 0$. Probabilistic models for this problem suggest that $\#S_x$ should have size at most $C \log x$ as $x \to \infty$, and computer experiments support this, so that there seems room to spare in solving this problem. Nevertheless this problem seems very difficult, and the warning above applies to it, too.*

So we formulate an even weaker problem. Consider the full forward and backward orbit of $n = 8$, which is:

$$S_\infty := \{1 \leq n \leq x : \text{some iterate } g^{\circ k}(8) = n \text{ or some iterate } g^{\circ k}(n) = 8\}.$$

Then we ask:

1932 Subproblem 2. *Prove or disprove the assertion that the (full forward and backward) orbit S_∞ of 8 contains all sufficiently large integers $N \geq N_0$. This is the assertion there are only finitely many positive integers not in the full orbit of $n = 8$!*

This assertion seems absurd; nevertheless is an unsolved problem to show that it is false. **WARNING.** *At present Subproblem 2 seems just as intractable as the $3x+1$ problem!*

REFERENCES

[1] A. O. L. Atkin, "Comment on Problem 63-13", SIAM Review **8** (1966), 234–236.
[2] R. K. Guy, "Don't try to solve these problems!", Amer. Math. Monthly **90** (1983), 35–41. http://www.jstor.org/discover/10.2307/2975688?uid=3739256&uid=2&uid=4&sid=21102550539183.

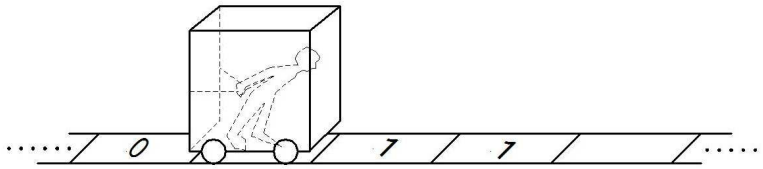

FIG. 1. *An artist's rendition of a Turing machine. Original drawing by wvbailey in Autosketch after Boolos and Jeffrey (1974, 1999) Figure 3-1, page 21, downloaded freely from Wikipedia.*

[3] M. KLAMKIN, "Problem 63–13", SIAM Review **5** (1963), 275–276.
[4] J. C. LAGARIAS, "The $3x+1$ problem and its generalizations", Amer. Math. Monthly **92** (1985) 3–23. http://mathramz.com/1/The_3x%2B1_Problem_and_Its_Generalizations.pdf.
[5] J. C. LAGARIAS, ED., "The Ultimate Challenge: The $3x+1$ problem", Amer. Math. Soc., Providence, RI 2011. D. Shanks, *Comments on Problem 63-13*, SIAM Review **75** (1965), 284–286.

1936

Alan Turing

Besides cracking codes at Bletchley Park during World War II and pioneering the field of artificial intelligence, Alan Turing might best be known for his eponymous model of computation, the Turing machine (see Figure 1). Consisting of an infinite tape partitioned into squares, the machine features a moving head that overlooks a single square at any moment in time. Squares start out blank but can also contain symbols from a finite alphabet. The head can read symbols from and write symbols to the tape. It also occupies one of n states-of-mind, which we simply call *states*. These states serve as the machine's memory. Computation occurs as follows: the head reads a symbol from its current square, writes a new symbol to the square (it might be the same symbol or a blank) and moves either to the left or to the right while also (potentially) changing its state. The alphabet, states, and transition rules constitute a finite description of a Turing machine.

In *On Computable Numbers, with an application to the Entscheidungsproblem*, Turing uses his machine to define a *Universal* machine—one that can take the description of another Turing machine as input and then simulate that Turing machine. It is the first example of the now ubiquitous virtual machine. Turing also uses his machine to define computable numbers, which are real numbers whose decimal values can be written down successively, with each additional digit appearing after a finite number of steps. These machines don't halt, but they always make progress. Most modern treatments of Turing machines deal with computable functions instead of computable numbers. In this scenario the computation begins with a tape initialized with some finite input. What remains on the tape after the machine halts is the output. Thus, computable functions are functions that can be computed by a Turing machine in a finite number of steps. Unlike the machines writing computable numbers, these machines always halt. A classic function that is not computable asks whether given the description of a Turing machine, will that machine halt on every input? This is called the the *halting problem* and it remains a natural gateway into the study of computability.

Though Kleene, Church, and Post had already developed models of computation that were equivalent in power, the Turing machine was the first to convince Kurt Gödel of what it truly meant to be an algorithm: *That this really is the correct definition of mechanical computability was established beyond any doubt by Turing.* Indeed, the Turing machine has remained the model of choice when explaining, extending or developing new concepts in computability and complexity theory.

Centennial Problem 1936. *Proposed by Brent Heeringa, Williams College.*

Suppose we restrict our attention to Turing machines with n states and one additional HALT state, which tells the machine to immediately cease computation. In addition, suppose these machines are only allowed to read and write 0s and 1s with 0s serving as the blank symbol, so the tape is initially all 0s. Let $\Sigma(n)$ be the maximum number of 1s appearing on the tape after any n-state Turing machine halts; $\Sigma(n)$ is called the *busy beaver function* and any n-state, halting Turing machine achieving $\Sigma(n)$ is called a *busy beaver*. It's clear that $\Sigma(n)$ is well-defined because there are only a finite number of n-state halting Turing machines over the binary alphabet $\{0, 1\}$. It is known that $\Sigma(3) = 6$ and $\Sigma(4) = 13$, but the exact value of $\Sigma(5)$ is unknown (it is at least 4098). As warm-up, show that $\Sigma(3) = 6$. Then show that, in general, $\Sigma(n)$ is not computable. Can you find any upper or lower bounds on its growth rate?

REFERENCES

[1] G. Boolos and R. Jeffrey, "Computability and Logic" (3rd edition), Cambridge University Press, Cambridge, UK 1999.
[2] K. G odel, "Undecidable Diophantine Propositions", in Collected Works III (from the 1930s), 164–175.
[3] T. Radó, "On non-computable functions", Bell System Technical Journal **41** (1962), no. 3, 877–884.
[4] A. M. Turing, "On Computable Numbers, with an application to the Entscheidungsproblem", Proceedings of the London Mathematical Society, 1942 Cambridge, New York, 2008. http://plms.oxfordjournals.org/content/s2-42/1/230. See the following link for a correction: http://plms.oxfordjournals.org/content/s2-42/1/230.

1940

A Mathematician's Apology

One of the most frequent pieces of good advice to newcomers in a field is to read the masters. There is something special about looking at Newton's Principia. Or reading Riemann's one and only paper on number theory, where his famous hypothesis is simply briefly mentioned as an aside. Of course, people who rise to the top often have other wisdom to impart than just their technical insights. One of the most important and time-consuming parts of an academic's job is to mentor the rising generation, just as the previous generation guided them. Numerous mathematicians through the ages have been very generous with their time. Fortunately, some have taken pen to hand and written extensively to share the lessons they've learned. One of the most prolific is Steven G. Krantz, whose titles include "A Mathematician's Survival Guide: Graduate School and Early Career Development", "A Primer of Mathematical Writing: Being a Disquisition on Having Your Ideas Recorded, Typeset, Published, Read & Appreciated", "How to Teach Mathematics ", "A Mathematician's Survival Guide: Graduate School and Early Career Development", "A TeX Primer for Scientists", and "The Survival of a Mathematician: From Tenure to Emeritus." These are terrific books, and give a nice sample of the issues, challenges and rewards that lie ahead (the last is available online [3]; all can be purchased for very reasonable amounts).

While there are many authors and texts to mention, this entry highlights G. H. Hardy's *A Mathematician's Apology*, first published in 1940 and available online [1, 2]. In it Hardy deals with a different issue. While many books discuss the challenges and rewards, his work is about his reflection on his life and whether or not it was well spent; mathematically it surely was, as Hardy is responsible for numerous advances and new techniques. The following are some passages; for those who are still trying to decide on a career, Hardy is asking us to consider *why* we should select a certain career below, and not *how* to do it well.

> *A man who sets out to justify his existence and his activities has to distinguish two different questions. The first is whether the work which he does is worth doing; and the second is why he does it (whatever its value may be). The first question is often very difficult, and the answer very discouraging, but most people will find the second easy enough even then. Their answers, if they are honest, will usually take one or other of two forms; and the second form is merely a humbler variation of the first, which is the only answer which we need consider seriously.*

> *(1) I do what I do because it is the one and only thing that I can do at all well. I am a lawyer, or a stockbroker, or a professional cricketer, because I have some real talent for that particular job. I am a lawyer because I have a fluent tongue, and am interested in legal subtleties; I am a stockbroker because my judgement of the markets is quick and sound; I am a professional cricketer because. I can bat unusually well. I agree that it might be better to be a poet or a mathematician, but unfortunately I have no talent for such pursuits.'*

> *A chess problem is genuine mathematics, but it is in some way 'trivial' mathematics. However ingenious and intricate, however original and surprising the moves, there is something essential lacking. Chess problems are unimportant. The best mathematics is serious as well as beautiful 'important' if you like, but the word is very ambiguous, and 'serious' expresses what I mean much better.*

> *My choice was right, then, if what I wanted was a reasonably comfortable and happy life. But solicitors and stockbrokers and bookmakers often lead comfortable and happy lives, and it is very difficult to see how the world is the richer for their existence. Is there any sense in which I can claim that my life has been less futile than theirs? It seems to me again that there is only one possible answer: yes, perhaps, but, if so, for one reason only.*

> *I have never done anything 'useful'. No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least*

difference to the amenity of the world. I have helped to train other mathematicians, but mathematicians of the same kind as myself, and their work has been, so far at any rate as I have helped them to it, as useless as my own. Judged by all practical standards, the value of my mathematical life is nil; and outside mathematics it is trivial anyhow. I have just one chance of escaping a verdict of complete triviality, that I may be judged to have created something worth creating. And that I have created something is undeniable: the question is about its value.

The case for my life, then, or for that of any one else who has been a mathematician in the same sense in which I have been one, is this: that I have added something to knowledge, and helped others to add more; and that these somethings have a value which differs in degree only, and not in kind, from that of the creations of the great mathematicians, or of any of the other artists, great or small, who have left some kind of memorial behind them.

Centennial Problem 1940. *Proposed by Steven J. Miller, Williams College.*

Read the masters! Pull up Riemann's original paper [4], or some article in a field that strikes your fancy. Read the rest of 'A Mathematician's Apology', or other similar books. Browse some math blogs. We're fortunate that we're in a time when the only cost of posting and publishing certain types of information is the time it takes to write it; the AMS has a great blog page for graduate students at http://blogs.ams.org/mathgradblog/, which has numerous links to blogs by mathematicians of all different interests (for example, if you click on the link to Theoretical Mathematics you'll find Terry Tao's blog, http://terrytao.wordpress.com/). Many people make career decisions by following paths of least resistance; really think about what you want to do. Don't just go with the flow; make as informed a decision as you can.

REFERENCES

[1] G. H. Hardy, "A Mathematician's Apology" (with a foreward by C. P. Snow), Cambridge University Press, 1967. https://ia600807.us.archive.org/26/items/AMathematiciansApology/Hardy-AMathematiciansApology.pdf.

[2] G. H. Hardy, "A Mathematician's Apology", First Electronic Edition, Version 1.0, March 2005, Published by the University of Alberta Mathematical Sciences Society. http://math.boisestate.edu/~holmes/holmes/A%20Mathematician's%20Apology.pdf.

[3] S. G. Krantz, "The Survival of a Mathematician: From Tenure to Emeritus", AMS 2008. http://www.math.wustl.edu/$\sim$sk/books/newsurv.pdf.

[4] B. Riemann, "On the Number of Prime Numbers less than a Given Quantity", Monatsberichte der Königlich Preuischen Akademie der Wissenschaften zu Berlin, 1859. http://www.claymath.org/sites/default/files/ezeta.pdf.

1944

Theory of Games and Economic Behavior

In 1944 von Neumann and Morgenstern published the book "Theory of games and economic behavior" [6], which became the seminal book in the field of game theory. Since its publication, game theory has steadily become more widely used both within and across disciplines. It is now perhaps the leading analytical tool in microeconomic theory, formal political theory, and evolutionary biology/ecology (see, e.g., [4] and [5]), and is now even used in the study of literature and philosophy [1]. One can easily argue that game theory is one of the great success stories of modern applied mathematics.

One of the central problems in the field is the determination of equilibrium strategies for rational participants, which range from existence questions (does an equilibrium exist, and if so, of what type) to normative ones (what is the optimal equilibrium). Enormous progress was made in 1950. In his Princeton mathematics dissertation [2], Nash proved that in a very large class of non-cooperative games, an equilibrium exists in which no player has an incentive to change her behavior; in his honor these points are now called Nash equilibria.

Nash's biography [3] was turned into a movie by the same name, *A Beautiful Mind*, which won the best picture Oscar in 2002. The movie dramatized the scene in which Nash thought of the idea for his thesis. Mathematicians, however, might get more of a kick out of a different scene, described in the book but left out of the movie, in which Nash visited von Neumann's office to share his idea. The book reports that the meeting was short, and ended with von Neumann saying "That's trivial, you know. That's just a fixed point theorem." The idea won Nash an Economics Nobel Prize in 1994.

Centennial Problem 1944. *Proposed by Daniel F. Stone, Bowdoin College, and Steven J. Miller, Williams College.*

The concept of a Nash equilibrium is simple: a set of (two or more) individuals is in Nash equilibrium if each individual's strategy is optimal, holding the others' strategies fixed; that is, if no single player has an incentive to unilaterally change her plan of actions. Unfortunately, the movie botched the illustration of this concept: in the movie scene mentioned above, Nash discovers the idea in a bar when he is with four male friends, and four brunette women and one blonde enter. Nash's (supposed) insight is that they should resist their temptation to each pursue the blonde. He suggests instead "what if no one goes for the blonde.... We don't get in each other's way.... That's the only way we win." He says this while imagining his four friends matching up with the four brunettes, with the blonde ignored, and himself excluded. See http://www.youtube.com/watch?v=CemLiSI5ox8.

To follow the movie's simplistic, dated structure, assume that matching with a brunette yields a positive payoff (for the male matched), matching with the blonde a higher payoff, and if a male matches with no one, then his payoff is zero. Assume also, as described in the movie, that if the male does not match with the first female he pursues, then he matches with no one, and that the probability of matching with a female pursued by n males is $1/n$. Suppose Nash is not a player in the game, as in the scene he pictures in the movie, so there are just four males, four brunettes, and one blonde. Why is the situation Nash pictures (in which each male pursues and matches with a brunette) not a Nash equilibrium? Under what conditions on the payoffs would it indeed (contrary to Nash's claim in the movie) be a Nash equilibrium for each male to pursue the blonde (and thus for 3 males to fail to match)? How might it matter (or not) if the males chose their actions simultaneously or sequentially? Last, return to simultaneous play by the males, and suppose the blonde might be more interested in some males than others. She can smile at a male to signal this interest, but her smile might also be incidental. Suppose a smile indicates a 0.75 chance of liking the male smiled at the most (otherwise, she likes each equally). Is it still possible for it to be a Nash equilibrium for each male to pursue the blonde? If so, under what conditions?

REFERENCES

[1] M. S.-Y. Chwe, "Jane Austen, Game Theorist", PrincetonUniversity Press, 2013.
[2] J. Nash, "Non-cooperative games", PhD Thesis, Princeton University, 1950. http://www.princeton.edu/mudd/news/faq/topics/Non-Cooperative_Games_Nash.pdf.

[3] S. Nassar, "A beautiful mind", Simon & Schuster, 1998.
[4] T. C. Schelling, "The strategy of conflict", Oxford University Press, 1960.
[5] J. M. Smith, "The theory of games and the evolution of animal conflicts", Journal of theoretical biology **47** (1974), no. 1, 209–221.
[6] J. Von Neumann and O. Morgenstern, "Theory of games and economic behavior", Princeton University Press, 1944.

1948

Elementary Proof of the Prime Number Theorem

The Prime Number Theorem (PNT) states that to first order the number of primes at most x is asymptotically $x/\log x$. First conjectured in the 1790s, it wasn't proved until almost 100 years later, when Hadamard and de la Vallée-Poussin independently proved it. They both approached the problem by using results from complex analysis to understand the distribution of zeros of the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$. This function makes sense for the real part of s greater than 1, and using the Fundamental Theorem of Arithmetic (every integer can be written uniquely as a product of primes) and the geometric series formula, we see it also equals $\prod_{p \text{ prime}} (1 - 1/p^s)^{-1}$ (this is called the Euler product; as the location of the integers is well-understood, by studying the sum over integers we can glean information about the primes). These proofs were unsatisfactory to many, as the PNT is a statement about integers, and it shouldn't be necessary to enter the complex plane for a proof. It took almost 50 years for an elementary (i.e., not using complex analysis) proof to be found by Erdös and Selberg.

Centennial Problem 1948. *Proposed by Steven J. Miller, Williams College.*

Chapter 1 of Aigner and Ziegler's *Proofs from THE BOOK* give six different proofs of the infinitude of primes. These include Euclid's proof, as well as ones using Fermat numbers, Mersenne numbers, and topology. Several of my favorites involve the Riemann Zeta Function. One of my favorites is that the irrationality of π^2 implies there are infinitely many primes. Prove this claim, and deduce from this a lower bound for how many primes are at most x. For another, consider $s = 1$ and use the divergence of the harmonic series $1/n$ to obtain another proof that there are infinitely many primes. With a bit more work, one can use that the growth rate of $\sum_{n \le x} 1/n$ is $\log x$ to estimate $\sum_{p<x} 1/p$ is about $\log\log x$.

REFERENCES

[1] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, Springer-Verlag, Berlin, 1998. See also http://arxiv.org/pdf/0709.2184 (spoiler: partial answers are there). Sadly, see also http://www.math.columbia.edu/~goldfeld/ErdosSelbergDispute.pdf.

1952

NSA Founded

Created by President Truman in 1952, the National Security Agency (NSA) is charged with the responsibility of protecting the nation's security. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce vital foreign intelligence information for U.S. policy makers and the U.S. military. A high technology organization, NSA is on the frontiers of communications and data processing.

The primary responsibility of mathematicians at NSA is to solve problems associated with signals intelligence and information security. In addition to the traditional area of cryptology, mathematicians at NSA work on problems in areas such as signal

analysis, speech processing, coding theory, data compression, analysis of communication networks and computer security – virtually every mathematical discipline finds some application within NSA!

Today, NSA is the country's largest employer of mathematicians, providing opportunities for both summer internships and full-time employment. The Director's Summer Program (DSP) and the Cryptanalysis and Exploitation Services Summer Program (CES SP) are summer internships open to undergraduate students majoring in mathematics, while the Graduate Mathematics Program (GMP) is a summer internship available to graduate students. Additionally, NSA hires full-time mathematicians and statisticians year-round at every degree level (bachelor's, master's, doctorate). For more information about these opportunities and how to apply, please visit www.nsa.gov/careers/.

Centennial Problem 1952. *Proposed by Proposed by NSA Cryptomathematics Institute.*

You are a cryptanalyst at Bletchley Park during World War II, assigned to work on decryption of strategic communications between German High Command and Army Group commanders. The underlying teleprinter code is a 32-symbol alphabet which represents the five-bit quantities 00000 through 11111. These teleprinter communications are encrypted with a device called the Schluesselzusatzgeraet 1940, codenamed TUNNY.

Very little is known about the TUNNY machine – it is believed to be a *key-additive* machine, meaning that ciphertext is the XOR of plaintext and key. TUNNY messages begin with a 12-letter message indicator, which has led to speculation that the encipherment process of the TUNNY machine involves 12 wheels. Further analysis of the message indicators collected over the last several months shows that the first eleven indicators take on 25 distinct values (every letter except `J`) while the last indicator only takes on 23 distinct values.

Recently, a significant breakthrough against TUNNY was obtained. Two messages with the same indicator were intercepted and it soon became apparent that they were slight variations on the same message. Arduous work by a colleague succeeded in reading this message, confirming that the TUNNY machine is in fact key-additive and producing a stretch of over 4000 key characters. Your job is to use these key characters to determine, as much as possible, how the TUNNY machine operates. The key file is reproduced below, using base-32 encoding `0-9,A-V`.

```
K5FSVEJ238VE49QT2DQP4P28J8ST6PGJ69GJPAA0MK99U9DM243OH8PN514N80G3
8Q58FTFHCUH61IVPOR2TGBITUTIV56KU56TVQ0V71CV8TMFSPM2HGOP228FGTSIM
3TSP8KHA7GG34QTCN83O7OP8JOJ450VS5J60EPMDUV70QPE5SHHS88A6OPIONQ08
V1KDULE9JG9KN4RLCKUL51MJ3AMMGBQDSMDUJESP0Q36G48E7SH2LA41TT29G4C5
NOF4TSIHC3I1OJ8JJDUPNO6UF2TUDURELMBQHHKDR7Q3CMOG44JEHADQUPID567O
P2N02I92H6DIFPCJKJTR30HQ718SH2PS3OB8RM6K4BCT08VC8NUPJ4B0365MHEQ8
1GJ4FG5LQ4AE3PCF1QL030NAE9PG0D4OSSRKDAVGJS1GBMQVVK7G919NLM7ETIBC
PA7OF3D1JAQ71UME1IHOEVR9MRLJEEB4C17LIC6TK9MGQHO1MHOHGJ25MPF6OU9E
LO4RVHVGGKVS5ANK2QOAPQJAH9DU4R5Q63878JQ5DUAKV4NQJCVOVC9KJC7T8GCM
J5TM9TVG76T194MT05SLKU20HFCVBTT6LQ18N80J0BIFCA5FBUPEFGBDRRCR0P2H
ALQ1PGI4EDRHIKKCNVQDM3FFA94EECOLEM3R2N4BMDOV2TUPEFTMKH3KHGLOFSLS
N26BE6SV762N3F8RA15TN8RO9A1IJ819HUOIL8NORDPCHD25MT81QT8JA0G3HHO1
APTKS8MJDH86TFQNFJU8SNJ83MLAFKR4PCFGF2MKK5OBCO3SR0RQ9QLEPUESOF4L
```

1LIPD6P8SK7RC9FDR6RTC0UCNFIF4R65KF2AIFMFSGM57TSJL9DQJLLQ0BJL27MK
RS9KIAL9EVIHQTKPEDOTO4LQ4FLDIL6T25916DVRABS88T7T8USI0ULUBGQQC7MU
DPNE45JUEOL6P9ERO78RO3UJ8JSF6DJ49AJO65IL6DDEHHHSTQ25K7K2SN2I7STQ
5DC8VCBC4PDHM46TG56T5BBO2VSR75I2DIG73NGT87UIAMF47VS86EL035HV52NE
HM1M72J092NG1ALMVVQRFS73K6O9ATGDAPQ1JHGQGU5J8JITG5C9JGJ49GFD580N
3121EBGRCFSJE8USS9KE7RA4O7Q6QG9UUM1Q4HK83K4G326OHSE50NOS4H6TM5I5
4LA8S74FLO4AFCDIALAF8338K5TG3KRKP6J5GJ2A491HU66JHVCAML0J4BI34761
2QE2L610RNM699MFG74CCUVCJKMB3K7QO9U9FUUSPSDKF0TK74P2R8SNDRCDNPUC
1L0K78NO5SN2H5MFJ7N8BE6I6A9EKTM96LNPO7L85UNC3SO9MT6HMDKLMLFJCJ9I
70LU34O4U1UPAG79VD2MUP8DQSO7874A096FCVB2QV2QOF0R2JGBM5UF6NN0FGN0
2P0R4TM93TPBIPB0VE8627ENR5NB0J23S3QK5CNO5EVC5UO3L92G6SD858CPQD8H
3D1QED6VL6L4UEBMPKUUVNSGI5OVVSG2JKB0RI92LM98H9UQM338B9ADGRADLAIP
AROKCE74NL6PT9VSPABODIBVSMM4JCFSLD2OM9OLRQKQF0OROV89ILE5JJ8OR8LD
6MUL69QE4B2GB2L30I29O5A9A90PUD0VM94RTNHIESP69QBED62R59G3ITNNBU1F
1I49ILEOCS7CRON2LUFKCFR969O4C8JGULTJB4RSTGRPSI48R8K42CSNRILAJLLE
740TF8GLS3MLL65SB0F8BCHMK1GKCD87I1ONETA5UF6Q9ELET75SR1H1AG3EJSL6
UU4PUD6SB1G16PALODQG2FI18NDMD0I1LS04VARF8K1FBV3CTQ1VGRNBFA9IPUB2
PI12VTQDSREHLUGMU1B2Q95QJA5Q92DKFO7DATD3DU6CI91SQ90H6DQLOHB8O3UL
07SJ4H65IDULCEU523I587U5CP25U8HJ9LQDER4BCHMHDJJA3DEE7S7C352TM9EO
5DRCFSD07GF2KNA530RI962646RHNG3ST43QSR2108CRC4VDF4B0DGBSR49GN09I
395RC1C8BCFSLPOD6P6M8JSBDPT54EU6BATF7TMTCTE5M7IV4RNO46JS7CVA5UM7
D9RMA83GH5EGK7AJ98JT5A1GA4NOK5PE8G4KF4H27AJKJSJQ5AHI1EJR8EIHOG3G
1AR4DATRR0NGBKQ056A3JOBIBNVJ4NCCUD2VCDAKAPS1QHQ58LMOFFDVO1SIO3A4
38NG2Q1EPPJEQ5SN2HK3TB1MDL7ME9G5ALM4HC745A6T8ATKT0BGR8JCDOFSR4HS
E6G2TSAK83S5HQM7C7EFO54EDPF9KNAP8BO7OPALULAACDUJGOODIPCK7HGVO38P
U95HSNVK9FFDSD2C0QR49UPADO3GS25N7A125AJG6IHM7K92L21HQ9VUNP5UVSB8
HSBOHOBMU5C1BHV8FKR3L47GVCL8BODIR831TQL4DUALA5K1PFS1ESAQLVOFTLV3
GHELA5U1CLI961GPUPDFU90JC3G129A2UO2C30U45PNCTVBI3QPR3EJVIUCLOFT4
CIV2TMJKTMF8K9IN47GNCU7FSSJ1SDA5OE0O56LEFRM3T64GCQAHSFPNGU9EM1S7
8NC12KA1ATS5ATUDST6C6N6RUHVR95QHA1UPKCIKUP3O2HVC93P1H4JB3E9U5E61
1A9E7UH66TL76HI5Q0PIRCNKSTU5ALQ9H37JLH9KK5EDAAO87S10NTMTDP6D9MF4
H6D6TS90IBFTOCJLFGLKA1CRQ1GJBK15R7VNHSVVFBGT68O7MI7T0BOF44RLUKML
C14DGJGU9OO4PQ3OF8Q3DFS51FMK83JCH4RP1L65OLH2KHFCFOJ8A06T6TK9QTGB
FAOPIRNM5MPE48M21ENR0M0KHNM2HEUHPRE16VAVA3GV47J6HHNKDIRKRGN2DICH
JLSG6G3H132PUDBP92HA5D9DA9PCJD0QHGBNE9OJ69VSFCNAPU1R4AMB808I4H69
GAFSDA59HO4N3MIHGUF3HKPCTALMILDBMKJ755JB0N63S70NACFTKB229RDFIR07
G3GJ1FGRNEJP6JR64OU5AMHDM9A9698PQ9ACDGUD9V2TSKOGNDC3RT85I70RO2J2
JM6120KJOJCHCLVG59L0IP7PKCU543IL0BSJCPQDIPNAPCULC5RE1QJ792HLVRER
4TOJIDC0JUVVMB44U98J9NKJOK31NG78PRU2LHNMFSK6V492GJ9G5TN83A1SJC6L
7TU9GQCTJ9LTADM56PGQVEHUPEFQT9QR9EVCC6TCGTDR0BUVB2V0L6NI7VETN102
THBOPUDOKD6P34G8KRUPGFAPQJH0MKBOL2FN4MSLSP942QHNQ9H9BO4JMJPL08V1
MFP3D2RK9IFU9MD0N5E4IL4NV0KBDSFCLEBN2N2TA96LB9NQ8DL65D8PU4T70CP7
CQSCCL4PI5GPIPUP09UJM2K2IO8RCDIJJ7O7AUQ9RS5IRU671CGOOPIJC03KJ85E
8C7O4TN5GF6T8B0V9KJCU5G44HI4RI5TIP9E2DORVILGGF7QMVUSC6JAVQD2DAV4
DM96TCB0GAEH15PH9QVUT2V8DHUNSFNL8V7P1J98JG3KS9QTORMHH9LBU830NO3O
5CN0BLPHTU37IL52KADKBC31A50N37MB6R77URIUHE1I5GNBGNO32JKB0J6FLA6S
5Q165EPBGV8FOR0QGDDODT75N2KR29A36E2TB03CH46SQOH0FGH27SLNR2D7IKMK
N5SG8VGBER340K197B6C9BHI83N3C2LM9RGCRK9QB5G7CFGOBDRGSLIRE548143C
1QV81QOR6MLAAB9PN6STR8L062FGLGTDJ03Q5T7165SP6DUTODJM2T54P6PQD9BU

```
NUQBVP5MOOJ4VDDCS4LQLIAKVO7KV4PCFKOJJ7GJQ9ORUO55DG7A5U1E77A2SN6N
VE6URPHND4VD67EHNGLKBORG5G2P47M947474LQ87P7SI4M52RIBGFP8PMO8IN3Q
```

Believe it or not, this is essentially how the solution of the TUNNY machine progressed in 1941–1942. On August 30, 1941, two TUNNY messages with the indicator `HQIBPEXEZMUG` were intercepted. Colonel John Tiltman recognized that these messages were *isologoues*, meaning that they were repeats of the same underlying plaintexts. Since the two messages had numerous typographical errors and extraneous spaces, the messages soon got out of sync with each other which allowed Tiltman to read both messages and recover a stretch of about 4000 key characters. In January 1942, William Tutte made a cryptanalytic breakthrough[1] that allowed him to ascertain the entire inner workings of the TUNNY machine.

Determining how TUNNY encipherment worked was just a single step towards producing an ability to read TUNNY messages from intercepted cipher. An excellent account of Bletchley Park's success against the TUNNY machine can be found in [1]. A technical report on TUNNY, written by the codebreakers themselves and containing a wealth of details about the machine and its exploitation, was declassified in 2000 and is available at [2].

REFERENCES

[1] J. Copeland et. al., "Colossus: The Secrets of Bletchley Park's Codebreaking Computers", Oxford University Press, New York, 2006.

[2] I. J. Good, D. Michie, and G. Timms, "General Report on TUNNY with Emphasis on Statistical Methods", available at www.alanturing.net.

1956

The GAGA Principle

In calculus one encounters a vast array of "transcendental" functions going beyond rational functions (for example, e^x, $\sin(x)$, $\log(x)$, etc.). In multivariable calculus with functions and differential geometry with smooth maps, the abundance of "transcendental" functions and maps becomes even more pronounced. Yet in 1956, it was shown by Jean-Pierre Serre (who had been awarded the Fields Medal in 1954) that in the setting of complex variables, under a compactness hypothesis many "transcendental-looking" geometric and function-theoretic constructions are *algebraic* from an appropriate point of view, and moreover that such an "algebraization" of the analytic construction is unique.

This result explained many earlier known special cases and was of fundamental importance in the development of algebraic and complex-analytic geometry. Not only did it justify in general the role of transcendental methods in the solution of algebraic problems admitting a sufficiently geometric flavor, but it inspired many new profound comparison results between algebraic and analytic constructions in the work of Grothendieck and others during the revolution that swept through algebraic geometry in the 1960's.

Serre's method of proof was sufficiently robust that it was later generalized to apply to geometric constructions over the p-adic numbers instead of $\mathbf{C}$, and this generalization is a ubiquitous tool in contemporary algebraic number theory. His 1956 paper is called "Géométrie algébrique et géométrie analytique", or GAGA for short, and the phrase "GAGA principle" expresses the idea that in the presence

[1] You'll need to find it for yourself!

of compactness, certain analytic constructions in geometry over $\mathbf{C}$ not only admit an algebraic description (which is already quite striking) but in fact an essentially unique one.

Centennial Problem 1956. *Proposed by Brian Conrad, Stanford University.*

This problem develops the classical content of Serre's theorem in the 1-dimensional case, assuming familiarity with undergraduate complex analysis.

Let f be a meromorphic function on $\mathbf{C}$. It is called *meromorphic at* ∞ if $f(1/z)$ is meromorphic at 0.

(i) Prove that every rational function $p(z)/q(z)$ for polynomials $p, q \in \mathbf{C}[Z]$ with $q \neq 0$ is meromorphic at ∞.

(ii) Prove that if f is meromorphic at ∞ then f is a rational function! (Hint: show f has only finitely many zeros and poles in $\mathbf{C}$, and use this to reduce to the case that f has no such zeros or poles. By studying the zero or pole order of $f(1/z)$ at $z = 0$, get to a case where Liouville's theorem can be applied.) Deduce that if a holomorphic automorphism $f : \mathbf{C} \to \mathbf{C}$ is meromorphic at ∞ then $f(z) = az + b$ for some $a \in \mathbf{C}^\times$ and $b \in \mathbf{C}$.

REFERENCES

[1] J-P. Serre, "Géométrie algébrique et géométrie analytique", Annales Fourier **6** (1956), 1–42.
[2] Wikipedia, "Algebraic and analytic geometry." http://en.wikipedia.org/wiki/Algebraic_geometry_and_analytic_geometry

1960

The Unreasonable Effectiveness of Mathematics in the Natural Sciences

This year honors a ground-breaking, influential article by Eugene Wigner, a Nobel laureate in physics whose work in random matrix theory eventually led to astonishing connections between the seemingly diverse fields of number theory (through zeros of the Riemann zeta function) and nuclear physics (through the energy spectra); see the entry from 1928 for more on this intereplay. In it he describes the use of mathematics in physics. To Wigner, mathematics is the science of skillful operations with concepts and rules invented just for this purpose. The principal emphasis is on the invention of concepts.

The entire article is available online (see the link in [2]), and worth reading. This quote from the article gives the reader a strong hint about the nature of the paper:

> *A possible explanation of the physicist's use of mathematics to formulate his laws of nature is that he is a somewhat irresponsible person. As a result, when he finds a connection between two quantities which resembles a connection well-known from mathematics, he will jump at the conclusion that the connection is that discussed in mathematics simply because he does not know of any other similar connection. It is not the intention of the present discussion to refute the charge that the physicist is a somewhat irresponsible person. Perhaps he is. However, it is important to point out that the mathematical formulation of the physicist's often crude experience leads in an uncanny number of cases to an amazingly accurate description of a large class of phenomena. This shows that the mathematical language has more to commend it than being the only language which we can speak; it shows that it is, in a very real sense, the correct language.*

Mathematics is often called the language of the universe, though some dispute how far the universe extends beyond physics and astronomy, and how much is needed to describe the world and make significant contributions. See for example the article [3] by the famous biologist E. O. Wilson, and then do a quick websearch for the heated responses and discussions that ensued. It is particularly fitting that this problem is appearing in the same congruence class as the 1984 entry, which provides additional reading on how language can shape our understanding of the world we inhabit.

Centennial Problem 1960. *Proposed by Stanislav Molchanov and Harold Reiter, UNC Charlotte.*

The following four problems illustrate the fundamental idea by Wigner on the applicability of a single mathematical fact to completely different areas of the knowledge.

Problem 1: Call $c_n = \frac{1}{n+1}\binom{2n}{n}, n \geq 1$ the Catalan numbers; note $c_1 = 1, c_2 = 2, c_3 = 5, \ldots$. Prove that $c_n, n \geq 1$ in an integer.

Problem 2: Consider the probability density

$$p(x) = \begin{cases} \frac{1}{2\pi}\sqrt{4-x^2} & \text{if } |x| \leq 2 \\ 0 & \text{otherwise} \end{cases}$$

(it is the density in Wigner's famous semicircle law, which he proposed for the description of the spectra of the heavy nuclei). Calculate the moments

$$m_{2k} = \int\limits_{R^1} p(x) \cdot x^{2k} dx = \frac{1}{2\pi} \int\limits_{-2}^{2} \sqrt{n-x^2} x^{2k} dx, \quad k \geq 1$$

(note that clearly we have $m_0 = 1$ and $m_{2k-1} = 0$ for $k \geq 1$).

Problem 3: Calculate the number t_n of the trees (graphs without cycles) containing n edges and the fixed root.

Problem 4: Assume we must multiply n symbol $a_1, a_2, \ldots a_n$ $(n \geq 2)$ using a binary but not necessarily associative operation $b(x, y)$, and thus we must keep track of order. We are interested in the number of structurally different ways we can combine the symbols, and not the number of different ways we can then input the n objects into the possibilities. Thus if we let S_{n-1} denote the number of different structures we can use to multiply n symbols using our binary operation $n-1$ times, we have $S_1 = 1$ as the only way to combine two symbols is $b(a_1, a_2)$; note we are not counting $b(a_2, a_1)$ as structurally it is the same as $b(a_1, a_2)$.

Continuing we see $S_2 = 2$ as we have $b(a_1, b(a_2, a_3))$ and $b(b(a_1, a_2), a_3)$, while $S_3 = 5$ as we have $b(b(a_1, a_2), b(a_3, a_4))$, $(b(b(a_1, a_2), a_3), a_4)$, $b(a_1, b(b(a_2, a_3), a_4))$, $b(b(a_1, b(a_2, a_3)), a_4)$, $b(a_1, b(a_2, b(a_3, a_4)))$.

Note: an alternative interpretation of S_n is that it is the number of ways to write down n let parentheses and n right parentheses so that, as we move from left to right, we have never seen more right parentheses than left parentheses. Thus for $n = 1$ we find S_1 is 1, as the only possibility is (), while for $n = 2$ we see $S_2 = 2$ as we have ()() and (()). Continuing, for $n = 3$ we calculate that $S_3 = 5$, with the five options ((())), (()()), (())(), ()(()), ()()(). If we interpret (as moving up one unit and) as moving

down one unit, it is the number of paths such that we never fall below our starting point as we walk.

Determine S_n.

REFERENCES

[1] A. Gelfert, "Applicability, Indispensability, and Underdetermination: Puzzling over Wigner's 'Unreasonable Effectiveness of Epiudom12345

[2] E. Wigner, "The Unreasonable Effectiveness of Mathematics in the Natural Sciences", Communications in Pure and Applied Mathematics, **13**, No. I (February 1960). https://www.dartmouth.edu/~matc/MathDrama/reading/Wigner.html

[3] E. O. Wilson, "Great Scientist ≠ Good at Math: E.O. Wilson shares a secret: Discoveries emerge from ideas, not number-crunching", essay published online in the Wall Street Journal, April 5, 2013 10:07 p.m. ET. http://www.wsj.com/articles/SB10001424127887323611604578398943650327184.

1964

The Principles of Mathematical Analysis

Many of the entries here have, rightly, honored major discoveries and advancements; however, in doing so there is a danger of overlooking other extremely valuable moments in mathematics. One of the most important contributions someone can make to the subject is to encourage, nurture and support others to join and thrive in the field. While there are many ways to do this, one of the best is through writing. The reason is that a good textbook or article can circle the globe, edition after edition, reaching generation after generation.

One of the most prestigious prizes honoring such work is the The Leroy P. Steele Prize for Mathematical Exposition. It was first given in 1993 to Walter Rudin for, among other contributions, his enormously influential books *Principles of Mathematical Analysis* [1] and *Real and Complex Analysis* [2]. To give a sense of the impact and influence these books have had, if you say 'blue book' or 'baby Rudin' most mathematicians immediately know you are talking about the first, while saying 'green book' or 'Papa Rudin' gives a smiling nod on the second. These books have been used in classes around the world for decades, where they have influenced numerous mathematicians. They have survived into many editions; in fact, the reason this is the entry for 1964 and not 1953 is that this year marks the publication of the second edition of *Principles*, and gives a sense of the staying power of the work.

Centennial Problem 1964. *Proposed by Steven J. Miller, Williams College.*

One of the reasons so many people love these books are the challenging problems collected at the end of chapters. On a personal note, I remember using the third edition of *Principles* as a sophomore at Yale. At the time I was on the fence between mathematics and physics, and the joy of wrestling with the problems here is what finally pushed me to the math camp. All these years later, I still remember problems 16, 17 and 18 from Chapter 3. This was my first introduction to Newton's method, and I remember being amazed at being able to prove how rapidly convergence set for square roots in problem 16 (problem 17 was a significantly slower method for finding square roots, and problem 18 was the generalization to problem 16 for p^{th} roots), and going to my instructor's office (Peter Jones) to talk about these further. So, while the problem below is somewhat standard, I've chosen to use that because of the impact these three problems had on me; I strongly urge any reader not familiar with these books to pick up a copy, read on, and try your hand at the exercises.

Exercise #16, Chapter 3 (third edition): Fix a positive number α. Choose

$x_1 > \sqrt{\alpha}$, and define $x_2, x_3, x_4, \ldots$ by the recursion formula

$$x_{n+1} \;=\; \frac{1}{2}\left(x_n + \frac{\alpha}{x_n}\right).$$

(a) Prove that $\{x_n\}$ decreases monotonically and that $\lim x_n = \sqrt{\alpha}$.
(b) Put $\epsilon_n = x_n - \sqrt{\alpha}$, and show that

$$\epsilon_{n+1} \;=\; \frac{\epsilon_n^2}{2x_n} \;<\; \frac{\epsilon_n^2}{2\sqrt{\alpha}}$$

so that, setting $\beta = 2\sqrt{\alpha}$,

$$\epsilon_{n+1} \;<\; \beta\left(\frac{\epsilon_1}{\beta}\right)^{2^n} \qquad (n = 1, 2, 3, \ldots).$$

(c) This is a good algorithm for computing square roots, since the recursion formula is simple and the convergence is extremely rapid. For example, if $\alpha = 3$ and $x_1 = 2$, show that $\epsilon_1/\beta < 1/10$ and that therefore

$$\epsilon_5 \;<\; 4 \cdot 10^{-16}, \qquad \epsilon_6 \;<\; 4 \cdot 10^{-32}.$$

REFERENCES

[1] W. Rudin, "Principles of Mathematical Analysis", McGraw-Hill, New York, 1953.
[2] W. Rudin, "Real and Complex Analysis", McGraw-Hill, New York, 1966.

1968

Atiyah-Singer Index Theorem

In the book Men of Mathematics [3], the author E. T. Bell describes the French mathematician Jules Henri Poincaré as the last Universalist. This account comes from the fact that, until the late 19th century, mathematics as a field had not diverged into the many different subjects that are presently explored in modern times. Specializations that range from the study of set theory to the furthest abstractions of algebra and analysis now carry the notion of self-containment with only a vague semblance of interdependence.

Finding unification between two or more of these contemporary mathematical subjects is a task that requires non-intuitively deep insight. In 1968, two mathematicians, Sir Michael Atiyah and Isador Singer, published work [1, 2] providing such insight that fused aspects of Topology with that of Analysis. Their result is known as the Atiyah-Singer Index Theorem. Basically, the theorem states that the analytical index is equal to the topological index. The mathematician I. M. Gelfand was the first to conjecture this notion in 1960. Rogues [6] summarizes the theorem in the conclusion of his paper by stating, "The Atiyah-Singer Index Theorem is a purely mathematical result. It tells us that a fundamental question in analysis, namely how many solutions there are to a system of differential equations, has a concrete answer in topology. This insight provides a short-cut to getting to know whether such solutions exist or not."

As differential equations are used to model physical dynamics, it is interesting to note that a pure mathematical field can determine the existence of their solutions. It is also interesting that the bridge Atiyah and Singer provided between analysis and topology has had a profound impact in the field of theoretical physics. Indeed, the

Atiyah-Singer Index Theorem has paved new paths connecting physical theories such as string theory with pure abstractions found in topology. It is keen results such as this that aid in understanding beyond the shroud of self-containment and reveal insightful connections that help make logical sense of the physical Universe.

Centennial Problem 1968. *Proposed by Avery T. Carr, Emporia State University, and Steven J. Miller, Williams College.*

At its heart, the Atiyah-Singer index theory says that two different quantities are equal, and if you can determine one then you can use that to answer problems in the other field. While a true example of their theorem would require some notation, there are problems similar in spirit that can be easily stated. We describe one of these now, the Catalan numbers; we chose this for our example as there are many different places in mathematics where these numbers arise (over 50 such occurrences are discussed in [7]), and we saw them in the entry for 1960.

One of the most common definitions of the Catalan numbers $\{C_n\}$ is that C_n is the number of ways to place n left parentheses and n right parentheses such that they are correctly matched; in other words, as we traverse our string we are never at a point where we have seen more right than left parentheses. For example, if $n = 2$ the possibilities are just (()) and ()(), while if $n = 3$ we have ((())), (())(), ()(()), (()()) and ()()(). The first few Catalan numbers are 1, 2, 5, 14, 42 and 132, and $C_n = \frac{1}{n+1}\binom{2n}{n}$. Other equivalent definitions include (i) the number of paths on a grid with $n \times n$ square cells starting at the bottom left, ending at the top right, and never going above the main diagonal, (ii) the number of ways a regular $(n + 2)$-gon can be divided into triangles by connecting vertices with non-intersecting lines, (iv) the number of permutations of $\{1, \dots, n\}$ that avoid any specified pattern of length three, as well as (v) the number of rooted binary trees with $n+1$ leaves and n internal nodes

Prove that C_n, defined combinatorially above, is also equal to

$$\lim_{x \to 0^+} n! \frac{d^n}{dx^n} \frac{1 - \sqrt{1 - 4x}}{2x}.$$

For more on the Catalan numbers, see the entry from 1960.

REFERENCES

[1] M. F. Atiyah and I. M. Singer, "The Index of Elliptic Operators I", Annals of Mathematics **87** (1968), no.3, 484–530.

[2] M. F. Atiyah and I. M. Singer, "The Index of Elliptic Operators III", Annals of Mathematics **87** (1968), no. 3, 546–604.

[3] E. T. Bell, "Men of Mathematics", Simon and Shuster (1937), 526–554.

[4] R. B. Melrose, "The Atiyah-Patodi-Singer index theorem", Research Notes in Mathematics, A. K. Peters, Ltd., Wellesley, MA, 1993. http://www.maths.ed.ac.uk/~aar/papers/melrose.pdf.

[5] Mathoverflow, "Intuitive explanation for the Atiyah-Singer index theorem", http://mathoverflow.net/questions/23409/intuitive-explanation-for-the-atiyah-singer-index-theorem.

[6] J. Rognes, "On the Atiyah-Singer index theorem", http://www.abelprize.no/c53865/binfil/download.php?tid=53804.

[7] R. P. Stanley, "Enumerative combinatorics. Vol. 2", Cambridge Studies in Advanced Mathematics **62**, Cambridge University Press, 1999.

[8] Wikipedia, "Atiyah-Singer index theorem", http://en.wikipedia.org/wiki/Atiyah%E2%80%93Singer_index_theorem.

[9] Wikipedia, "Catalan number", http://en.wikipedia.org/wiki/Catalan_number.

1972

Zaremba's Conjecture

In the 1950's and 1960's, people began studying algorithms for numerical integration in several variables. For simplicity, suppose we wish to numerically estimate the integral of a smooth function of two variables over a unit square. All a computer can do is average the value of the function at a finite number, say q, of sample points. In 1971, Zaremba observed that a particularly good choice of sample points are obtained by choosing pair of coprime integers p and q and sampling at the points $(n/q, np/q \bmod 1)$, as n ranges from 1 to q (thus giving q sample points). The quality of the approximation depends on how small the partial quotients a_j are in the(finite) continued fraction expansion of $p/q = [a_1, a_2, \ldots, a_k]$. In 1972, Zaremba conjectured that this "height" can be made absolute, for any choice of sample size q.

Centennial Problem 1972. *Proposed by Alex Kontorovich, Yale University.*

For each positive integer A let $\mathcal{D}_A$ be the set of all positive q such that there is a reduced rational p/q with p and q relatively prime whose continued fraction expansion $p/q = [a_1, a_2, \ldots, a_k]$ has partial quotients a_j bounded by A (see [2, 3] for a quick introduction to continued fractions). Prove that there exists a number $A > 1$ with $\mathcal{D}_A$ equal to the set of all positive integers. Bonus points: Prove that $A = 5$ suffices. Extra extra bonus points: Prove that $A = 2$ suffices, if a finite number of integers are allowed to be omitted.

REFERENCES

[1] J. Bourgain and A. Kontorovich, "On Zaremba's Conjecture", http://arxiv.org/abs/1103.0422.

[2] S. J. Miller and R. Takloo-Bighash, "An Invitation to Modern Number Theory", Princeton University Press, Princeton, NJ, 2006, 503 pages.

[3] A. J. van der Poorten, "Notes on Continued Fractions and Recurrence Sequences", Number theory and cryptography (Sydney, 1989), 86–97, London Math. Soc. Lecture Note Ser. **154**, Cambridge Univ. Press, Cambridge, 1990. http://maths.mq.edu.au/~alf/www-centre/alfpapers/a094.pdf.

1976

Four Color Theorem

The year 1976 marked the end of the long search for proof of the Four Color Theorem, initially proposed in 1852 by Francis Guthrie. The theorem states that any fully colored map (a plane separated into contiguous regions) requires only four colors to ensure that no adjacent regions are the same shade; see Figure 2 for an example. Guthrie's conjecture was specifically prompted by his attempt to color a map of the counties of England, and today most people know the theorem in the form "no more than four colors are needed to color a map." Despite this common understanding of the theorem, mapmakers claim it doesn't actually matter much to them, because usually there is no reason to limit colors, and if restricted, usually only three colors are actually needed. Despite its pragmatic insignificance, the problem has great historical importance.

The Four Color theorem has the dubious honor of having been proven twice before 1976 – incorrectly. Each earlier proof, one by Alfred Kempe in 1879 and one by Peter Guthrie Tait in 1880, stood unchallenged for 11 years before flaws were found. It was not until 1976 that mathematicians claimed again to have solved the elusive theorem, and even so, their claim was controversial.

Kenneth Appel and Wolfgang Haken at the University of Illinois proved the Four Color Theorem using computer assistance, through which they could simplify the infinite cases into 1,936 specific cases, which were each then checked by hand. As the first proof to rely on extensive computer assistance, this was greeted with controversy

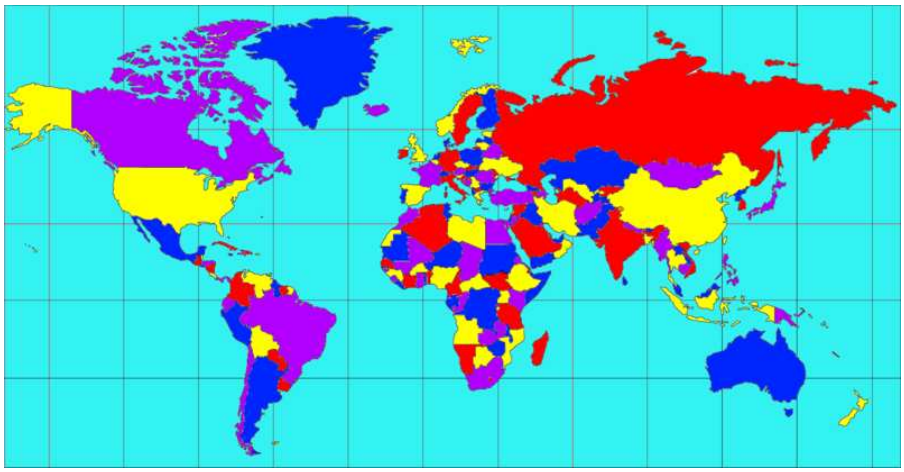

FIG. 2. *A coloring of the nations of the world using just four colors; can you figure out what year this map is from? Image courtesy of user Ameoba5 from Wikimedia Commons.*

from the mathematical community (for another proof generating even more discussion, see the Kepler Conjecture entry from 1998). What does it mean to not be able to see the functioning of the proof, to instead have to believe that technology computed correctly? Is such a proof as valid as one where one can see how it moves from step to step, from beginning to end? Mathematicians decided that such a method is valid (don't worry, this proof hasn't been disproven yet!), but that certainly doesn't mean a proof where almost 2,000 things have to be hand-checked is elegant. The elegant proof of the Four Color Theorem is still to come, so watch out, or try yourself.

Centennial Problem 1976. *Proposed by Alexandra Jensen, Steven J. Miller and Pamela Mishkin, Williams College.*

We know four colors suffice to ensure that all nations on a map can be colored so that no two sharing a border are colored the same (note that we assume all nations are contiguous). What if we add the constraint that each color may not be used more than $p\%$ of the time? For what $p \in [.25, 1]$ must a four coloring exist? The four color theorem says we may take $p = 1$, and the Pigeon Hole Principle tells us we cannot do any $p < 1/4$. What if instead we only require at most $p\%$ is any color when there are at most N regions?

REFERENCES

[1] K. APPEL and W. HAKEN, "Every Planar Map is Four Colorable. Part I. Discharging", Illinois Journal of Mathematics **21** (1977), 429–490. http://www.projecteuclid.org/euclid.ijm/1256049011.

[2] K. APPEL, W. HAKEN and J. KOCH, "Every Planar Map is Four Colorable. Part II. Reducibility", Illinois Journal of Mathematics **21** (1977), 491–567. http://projecteuclid.org/euclid.ijm/1256049012.

[3] K. APPEL and W. HAKEN, "Solution of the Four Color Map Problem", Scientific American **237** (1977), no. 4, 108–121, doi:10.1038/scientificamerican1077-108.

[4] K. APPEL and W. HAKEN, "Every Planar Map is Four-Colorable", American Mathematical Society (1989), Providence, RI.

[5] G. GONTHIER, "Formal ProofThe Four-Color Theorem", Notices of the American Mathematical Society **55** (2008), no. 11, 1382–1393. http://www.ams.org/notices/200811/tx081101382p.pdf/

[6] R. THOMAS, "An Update on the Four-Color Theorem", Notices of the American Mathematical Society **45** (1998), no. 7, 848–859. http://www.ams.org/notices/199807/thomas.pdf.

[7] Wikipedia, "Four color theorem", http://en.wikipedia.org/wiki/Four_color_theorem.

1980

Dehn Invariants

At the International Congress of Mathematics in Paris in 1900, David Hilbert presented 10 problems to inspire and guide mathematicians in the new century; later 23 were published. These problems greatly shaped mathematics in the twentieth century; an English version is available here:

http://www.ams.org/journals/bull/1902-08-10/S0002-9904-1902-00923-3/S0002-9904-1902-00923-3.pdf.

His third problem concerns polyhedra (which are the analogues of polygons in three dimensions). Hilbert asked if we had two polyhedra with equal volumes whether or not one could be cut into finitely many polyhedra which could then be reassembled to give the second. By introducing an invariant (this is a quantity which is unchanged by cutting), Dehn proved in 1901 that the answer is no as the cube and the tetrahedron have different values. More is true. Later Debrunner showed that if a polyhedra tiles three-dimensional space then its Dehn invariant is zero; as tetrahedra have non-zero Dehn invariants this means they cannot tile.

Centennial Problem 1980. *Proposed by Jeffrey Lagarias, University of Michigan.*

Problems on packing and tiling go back to antiquity. In his work *On the Heavens*, Aristotle made an assertion (Book 3, sec. 8) that "regular tetrahedra fill their place", which is taken to mean they locally fill space. This is not so, and they cannot completely fill space around a single point. This leads to the following problem, which is unsolved. How many non-overlapping congruent regular tetrahedra can touch a point in $\mathbb{R}^3$?

One can show that 20 tetrahedra can touch at a point. This can be done in such a way that the 20 opposite faces of these tetrahedra (not touching the point) lie on the 20 faces of a regular icosahedron, whose centroid is the point where the tetrahedra touch. We can get an upper bound on how many tetrahedra can touch by determining the solid angle subtended by a regular tetrahedron, and dividing it into a full solid angle is $4\pi \approx 12.56$ steradians. In this way it is found there is room for at most 22 tetrahedra to touch at a point. Is the answer 20, 21 or 22? No one knows. The answer is suspected to be 20. Can one even rule out 22? The problem can be turned into a two-dimensional problem, by intersecting with a small sphere. It asks: *How many equilateral spherical triangles, with all angles* $\arccos(1/3)$ *(about* 71 *degrees) can be packed on the surface of a unit sphere without overlap?*

REFERENCES

[1] J. C. Lagarias and C. Zong, "Mysteries in Packing Regular Tetrahedra", Notices Amer. Math. Soc. **59** (2012), No. 11, 1540–1549. http://www.ams.org/notices/201211/rtx121101540p.pdf.

1984

For this entry, the year is the title. Here 1984 refers to George Orwell's classic dystopian novel, 1984. Written thirty-five years earlier, it describes a world in perpetual war where the three major governments manipulate and control their populations. Some of the methods are centuries old, such as informants, constant surveillance and fear; others are either new or are given a clearer expression than before, such as

Newspeak (the language of Oceania, designed to *limit* freedom of thought by restricting what can be discussed).

One of the most famous passages of the work involves the equation $2 + 2 = 5$. The protagonist, Winston Smith, is thinking about Big Brother and the rule of the party.

> *In the end the Party would announce that two and two made five, and you would have to believe it. It was inevitable that they should make that claim sooner or later: the logic of their position demanded it. Not merely the validity of experience, but the very existence of external reality, was tacitly denied by their philosophy. The heresy of heresies was common sense. And what was terrifying was not that they would kill you for thinking otherwise, but that they might be right. For, after all, how do we know that two and two make four? Or that the force of gravity works? Or that the past is unchangeable? If both the past and the external world exist only in the mind, and if the mind itself is controllable what then?*

.

A few paragraphs later, the chapter ends with Winston thinking:

> *Freedom is the freedom to say that two plus two make four. If that is granted, all else follows.*

The other entries of this work honor mathematicians, or mathematical events; in a sense, this year honors math itself!

Centennial Problem 1984. *Proposed by Steven J. Miller, Williams College.*

In honor of Winston's thought on everything following from the freedom to say $2+2 = 4$, this year's problem is the famous Four Fours puzzle: given four fours and an unlimited number of a finite set of mathematical operations, which natural numbers are constructible? For example, $44 - 44 = 0$, $44/44 = 1$, $4/4 + 4/4 = 2$, while for 49 we could use $4! + 4! + 4/4$. There are numerous versions of this problem online; a little searching online led me to [1], which posted the following formulation from "The Great International Math on Keys Book" [3]:

> Here's a brain teaser! Can you (with the help of your calculator, as needed) "build" all the whole numbers between 1 and 100 using only four 4's? Use only the + - X / ( ) . ^2 = and 4 keys on your calculator. 4!=4X3X2X1 is allowed, along with repeating decimal 4 (.4∼=.4444...). The first 8 are shown below. (All the whole numbers up to 120 have been "built" with just four 4's - how many can you find?)

As mentioned above, there are lots of different versions of this where different operations are or are not allowed; for example, more advanced calculators have lots of special function key, ranging from hyperbolic trigonometric functions to combinatorial ones. As we are allowed to repeatedly apply functions to expressions, it may be possible to represent all such numbers. Therefore, to make the problem even more interesting, let's add a scoring component. Assign a cost of 1 unit to the four basic

binary operations (addition, subtraction, multiplication and division). Continuing, assign a cost of 2 units for exponentiation, factorization, and n^{th} roots. Continue along these lines until you have assigned a value to all the operations you are allowed to use. Classify all numbers of cost at most C. Given some integer n, is there a bound on the minimal cost to represent it?

REFERENCES

[1] P. Karsanow, "Four Fours FAQ", copyright 1997–2005, http://www.oocities.org/hentaihelper/44sfaq.htm.
[2] G. Orwell, "Nineteen Eighty-Four. A novel", London: Secker & Warburg.
[3] Texas Instruments Incorporated, "The Great International Math on Keys Book", Texas Instruments, 1976.

1988

Mathematica

On June 23, 1988, Mathematica 1.0 is launched. The following quote is from its website; see [2, 3, 6] for more on the program and its first twenty-five years.

> *It is often said that the release of Mathematica marked the beginning of modern technical computing. Ever since the 1960s individual packages had existed for specific numerical, algebraic, graphical, and other tasks. But the visionary concept of Mathematica was to create once and for all a single system that could handle all the various aspects of technical computing–and beyond–in a coherent and unified way. The key intellectual advance that made this possible was the invention of a new kind of symbolic computer language that could, for the first time, manipulate the very wide range of objects needed to achieve the generality required for technical computing, using only a fairly small number of basic primitives.*

Centennial Problem 1988. *Proposed by Steven J. Miller, Williams College.*

If you've never used Mathematica before, the best possible problem is to go to its webpage and try it out. See [4] for a quick online tutorial from the company (or see Miller's homepage [1] for a template and video; the video is also available on YouTube at http://www.youtube.com/watch?v=g1oj7CIqGM8). For more on what it can do, check out the demonstrations page [5].

REFERENCES

[1] S. J. Miller, "Some quick links and files for LaTeX and using Mathematica", http://web.williams.edu/Mathematics/sjmiller/public_html/math/handouts/latex.htm.
[2] Wolfram, "The History of Mathematica", http://www.wolfram.com/company/mathematica-history.html.
[3] Wolfram, "The Mathematica Story: A Scrapbook", http://www.mathematica25.com/.
[4] Wolfram, "Watch a quick overview of Mathematica", http://www.wolfram.com/common/includes/m9videos/quicktour.html?KeepThis=true&TB_iframe=true&width=556&height=338.
[5] Wolfram, "Wolfram Demonstrations Project", http://demonstrations.wolfram.com/.
[6] S. Wolfram, "There Was a Time before Mathematica... June 6, 2013", Stephen Wolfram Blog, http://blog.stephenwolfram.com/2013/06/there-was-a-time-before-mathematica/.

1992

Monstrous Moonshine

Monstrous Moonshine refers to a connection between the theory of modular functions and the monster group investigated by John Conway and Simon Norton in 1979. The monster group is a finite simple group of order $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot$

$23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53}$, where simple just means that it has no interesting normal subgroups (i.e., its only normal subgroups are itself and the identity). It is one of only 26 sporadic finite simple groups. The connection between the monster group and modular functions is that the terms in the Fourier expansion of Klein's j-invariant (a modular function, and the only modular function f in a subclass of modular functions satisfying $f(e^{\frac{2}{3}i\pi}) = 0$ and $f(i) = 1728$) can be written as linear combinations of the dimensions of representations of the monster group. The first few terms of the Fourier expansion are as follows:

$$j \;=\; q^{-1} + 744 + 196884q + 21493760q^2 + \cdots,$$

where $q = e^{2\pi i\tau}$ and τ is the half period ratio. As an example of the connection, $196884 = 196883 + 1$, and 196883 is the degree of one of the representations of the Monster group. The later terms are also simple linear combinations of the character degrees of the Monster group. This similarity is highly fascinating simply because the coefficients are so large that a coincidence is an unlikely explanation.

The discovery of the similarity between this function and the Monster group led to the discovery of several other similar connections between modular functions and group theory. Richard Borcherds thought of the proof of the relationship in 1992 and won the fields medal for his proof. One of the main elements of his proof was to construct a $\mathbb{Z}^2-$graded Lie algebra on which the Monster acts. As a result of his proof, the relationship between the two mathematical objects is now understood as follows: there is a vertex operator algebra called the *Moonshine Module* which has the Monster as an automorphism group and the j-invariant as its graded dimension.

The name of the connection refers in part to the monster group, and "moonshine" comes from John Conway's reaction to the connection; he called the possibility of such a relationship "moonshine" as it seemed so improbable. The underlying similarities of the two seemingly unrelated topics comes from conformal field theory (field theory that is invariant under conformal transformations), a theory that is used in modeling statistical mechanics, string theory, and condensed matter physics.

Centennial Problem 1992. *Proposed by Blake Mackall and Steven J. Miller, Williams College.*

It takes awhile to truly appreciate numbers of the size of the Monster group. For example, there are 26! substitution ciphers in cryptography using the English language (in a substitution cipher, we write the re-ordered alphabet under the standard alphabet, which gives us a rule in how to replace letters); $26! \approx 4 \cdot 10^{26}$, which is slightly less than the *square-root* of the Monster's size!

It's fascinating that this particular number corresponds to the size of an interesting group. If we restrict ourselves to just the primes appearing in the factorization, we have fifteen primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71. How many distinct products of powers of these fifteen numbers exist which yield a number within a factor of 100 of the Monster's size? What if we instead allow ourselves to use all primes at most 71?

As big as the Monster is, its size pales in comparison to other quantities in mathematics, such as Graham's number. For an excellent introduction to the subject, see Graham's video [4] or a exposition by Lamb in Scientific American [5].

REFERENCES

[1] R. Borcherds, "Monstrous Moonshine and monstrous Lie superalgebras", Invent. Math. **109** (1992) 1–2, http://math.berkeley.edu/~reb/papers/monster/monster.pdf.

[2] J. H. Conway and S. P. Norton, "Monstrous Moonshine", Bull. London Math. **11** (1979) (3), 308–310.
[3] T. Gannon, "Monstrous Moonshine: The first twenty-five years", Bull. London Math. Soc. **38** (2006), no. 1, 1–33, http://arxiv.org/pdf/math/0402345v2.pdf.
[4] R. Graham and B. Haran, "How big is Graham's number?", https://www.youtube.com/watch?v=GuigptwlVHo.
[5] E. Lamb, "Graham's Number Is Too Big for Me to Tell You How Big It Is", Scientific American, April 1, 2014, http://blogs.scientificamerican.com/roots-of-unity/2014/04/01/grahams-number-is-too-big/.
[6] Wikipedia, "Monstrous moonshine", http://en.wikipedia.org/wiki/Monstrous_moonshine.

1996

Great Internet Mersenne Prime Search (GIMPS)

While we have known for millennia that there are infinitely many primes, far less is known about primes of special forms. For example, it is still an open question as to whether or not there are infinitely many primes (1) differing by two (though phenomenal recent progress has shown there is some even number $2m$ such that there are infinitely many primes whose difference is $2m$), or (2) of the form x^2+1, or (3) prime pairs (p,q) where $p=(q-1)/2$ (if q is an odd prime then $q-1$ must be divisible by 2, and thus $(q-1)/2$ being prime is the best we can hope for in studying $q-1$ for q prime; these are called Sophie Germain primes). It is believed that all of these sets of primes are infinite, though other interesting sets are expected to contain only finitely many primes, such as the Fermat numbers $F_n = 2^{2^n}+1$.

Why do we expect the first three sets to have infinitely many primes and the fourth not? The reason is the relative size of the sets. Notice the numbers F_n are growing so fast that their *logarithms* are growing exponentially! This set is far sparser than the others, and simple probabilistic heuristics suggest there are only finitely many. The Prime Number Theorem tells us that the number of primes up to x is approximately $x/\log(x)$; thus the probability a number n is prime is well-modeled by $1/\log(n)$. If we let X_n be a random variable that is 1 with probability $1/\log(n)$ and 0 otherwise, assuming independence the expected number of Fermat numbers that are also prime should be around $\sum_{n=0}^{\infty} 1/\log(F_n)$, which is about 2 or 3. We believe that the only Fermat numbers to be prime are the first five.

Thus, if we're looking for a set of numbers $\{a_n\}$ to contain infinitely many primes, there should be enough of them so that $\sum_n 1/\log(a_n)$ diverges. A natural candidate is to take $a_n = 2^n - 1$; we subtracted 1 as 2^n is clearly not prime. The sum giving the expected number is the harmonic series, which diverges, and thus there is cause for optimism. Unfortunately, there are arithmetic issues. Note that if n is composite then 2^n-1 is never prime (if $n=ab$ with $a,b\geq 2$ then $2^n-1=(2^a)^b-1^b$; we leave the completion of the factorization to the reader). What if we restrict n to the primes? In that case then sometimes 2^n-1 is prime (such as when n is 2, 3, 5, 7, 13, 17, 19 and 31), but sometimes it is not (such as when n is 11, 23 and 29). When 2^n-1 is prime we call the resulting number a Mersenne prime; we often write these as $M_p = 2^p-1$ with p prime. It is still an open question as to whether or not there are infinitely many Mersenne primes, though we believe there are and many results are known about them (perhaps the most famous connects Mersenne primes to perfect numbers: an even number is perfect if and only if it equals $(M_p+1)M_p$ for some Mersenne prime).

Though people had been investigating special p to determine the primality of certain Mersenne candidates for hundreds of years, with some success, a major advance happened in 1996. While most of the young readers of this article were still waiting

for AIM accounts to talk to SmarterChild, George Woltman turned on his cable modem and began an epic quest for Mersenne primes. Since 1996, much of the search for Mersene primes has been conducted as a collaborative project called the Great Internet Mersene Prime Search (GIMPS). It uses a set of software, Prime95 and MPrime, and a distributed architecture across multiple collaborating users. Thus far the project has identified fourteen Mersenne primes, bringing to 48 the number that have so far been identified. The largest one has 17,425,170 digits and is $M_{57,885,161}$. There is a prize of $150,000 for the first person or team who identifies a Mersenne prime of over 100 million digits.

The factoring code works in three phases to determine whether a number $2^p - 1$ is prime. First it creates a sieve of Eratosthenes to eliminate small factors, relying on the property that any factors must be of the form $f = 2kp + 1$ with $f = 1$ or 7 modulo 8, eliminating potential factors in this way eliminates about 95% of potential factors. Then $P - 1$ factoring searches for all factors with k less than some bound. Finally, GIMPS turns to the Lucas-Lehmer primality test.

Centennial Problem 1996. *Proposed by Steven J. Miller and Pamela Mishkin, Williams College.*

Like many years, 1996 was a particularly hard one to choose. There are frequently many good candidates; for 1996, it was neck and neck between GIMPS and PageRank. For most of us, PageRank is by far the more important of the two, and the better known (see [1] for one of the earliest papers, and then we leave it as an exercise to the reader to navigate and find out more!). While these are strong reasons to choose PageRank, in the end the deciding factor giving GIMPS the win was the simplicity of the potential question: *Find the next Mersenne prime!* Or, a little weaker, find a Mersenne prime not on the list.

REFERENCES

[1] S. Brin and L. Page, "The anatomy of a large-scale hypertextual Web search engine", Computer Networks and ISDN Systems **30** (1998), 107–117.
[2] C. K. Caldwell, "Mersenne Primes: History, Theorems and Lists", http://primes.utm.edu/mersenne/index.html.
[3] GIMPS Homepage, http://www.mersenne.org/.

2000

R

This year's choice deals with one of the most popular statistical programming languages and environments, R. Created by Ross Ihaka and Robert Gentleman at the University of Auckland, New Zealand in 1993, R is widely used in industry and academia around the world to perform statistical computations. As it is open source and freely available, there are numerous developers and thousands of useful packages. On February 29, 2000 marks version 1.0.0, the first version considered stable enough for general use.

Centennial Problem 2000. *Proposed by Steven J. Miller, Williams College.*

Years ago as a post-doc at Ohio State I attended a weekly data analysis seminar. One speaker (I sadly forget his name) gave a powerful talk on the issues of data analysis in the 21st century. Paraphrasing, he said that each day weather satellites beam down more information than is in the entire Library of Congress, and all this must be mined and processed in a matter of hours (or less!). To be scientifically literate these days one must both know statistics, as well as be able to write simple programs to cull and analyze data from the web. Download R and analyze a real

world problem. For example, look at all batters in baseball with bases empty and with just a runner on first and no outs; are the batting averages in the two cases statistically different? To solve this problem you will have to find online sites with baseball game data, reconstructing the games to get the game-state of each at-bat.

REFERENCES

[1] The R Project for Statistical Computing, http://www.r-project.org/.
[2] R (programming language), Wikipedia, http://en.wikipedia.org/wiki/R_(programming_language).

2004

Primes in Arithmetic Progression

We start our most recent decade with a beautiful theorem of Ben Green and Terence Tao. They proved that the set of primes contains arbitrarily long arithmetic progressions. What this means is that given any integer N there is some k such that $p, p+k, \ldots, p+Nk$ are all prime.

Their result is closely related to another problem, that of bounded gaps between primes, which states that given any even number $2m$ there are infinitely many pairs of primes whose difference is $2m$. For example, if $2m = 2$ we get the twin primes, the first few pairs being $(3,5)$, $(5,7)$, $(11,13)$ and $(17,19)$.

Centennial Problem 2004. *Proposed by Steven J. Miller, Williams College.*

Green and Tao's result immediately implies that given any integer N there is an even number $2m$, *where* $2m$ *is allowed to depend on* N, such that there are at least N pairs of primes whose difference is $2m$. Prove this result elementarily; in other words, show the existence of a $2m$ given N without appealing to Green-Tao.

REFERENCES

[1] B. Green and T. Tao, "The primes contain arbitrarily long arithmetic progressions", Annals of Mathematics **167** (2008), no. 2, 481–547. It is available online here: http://arxiv.org/abs/math.NT/0404188.

2008

100th Anniversary of the t-test

The Central Limit Theorem is one of the masterpieces of probability. It allows us to look at the sums or averages of many random variables sampled from an unknown distribution and make conclusions about the distribution of these sums or averages. This has powerful applications in statistics. It allow us to compare the average of a data set to a known distribution, the Gaussian, as long as we know the population's standard deviation, and allows us to set hypotheses on the value of certain key parameters. Unfortunately, in practice we often do not know the population's standard deviation, and using our sample's standard error introduces extra uncertainty into the model that must be taken into account.

In 1908, a brewer named W.S. Gossett working for Guinness ran into this problem when trying to analyze data on the best barley and hops to use in beer production. Gossett came up with a clever solution that revolutionized statistics: he added the error from the approximated standard deviation into the tails of the Gaussian model to create a new probability distribution that gave accurate estimates for the probability of the observations yielding a mean at least as extreme as the observed mean given the assumptions about the population mean. Gosset published the model under the pseudonym "Student" due to company policies at Guiness designed to limit other brewers from benefiting from statistical research its employees carried out. Explicitly

the model states:

$$\text{Prob}(X > x) \;=\; \frac{\Gamma(\frac{\nu+1}{2})}{\sqrt{\nu\pi}\Gamma(\nu/2)}(1+x^2/\nu)^{-\frac{\nu+1}{2}},$$

where $\Gamma(x)$ is the gamma function and ν is the number of degrees of freedom in the model, which is generally equal to the number of observations in the data minus 1. In application, a t-value, equal to the difference of the sample mean and hypothesized mean times the square root of the number of observations divided by the sample variance, is calculated and compared to the probabilities in this distribution.

A popular use of the Student's t-test is when looking at the correlation between two quantitative variables. Generally, a model for the data is picked so that the assumption that errors from the model are normally distributed is reasonable. However, since the regression might not be over many points, estimating the standard deviation of the errors introduces extra variance in the model, exactly what the Student's t-model is designed to do. The Student's t-model can also be used to compare the means of two populations and compare the mean of a population to a specified value. After 100 years, the Student's t-test is still one of the most widespread and celebrated tools in statistics.

Centennial Problem 2008. *Proposed by David Burt and Steven J. Miller, Williams College.*

The density of the Student t-distribution with ν degrees of freedom is

$$f_\nu(t) \;=\; \frac{\Gamma\left(\frac{\nu+1}{2}\right)}{\sqrt{\pi\nu}\,\Gamma\left(\frac{\nu}{2}\right)} \;\cdot\; \left(1+\frac{t^2}{\nu}\right)^{-\frac{\nu+1}{2}};$$

here ν is a positive integer, t is any real number, and $\Gamma(s)$ is the Gamma function, defined for $x > 0$ by

$$\Gamma(x) \;=\; \int_0^\infty e^{-t}t^{x-1}dt.$$

While the t-distribution was originally developed to investigate statistical problems, it turns out to have interesting applications in pure mathematics. Specifically, it can be used to prove Wallis' fascinating infinite product representation for π:

$$\frac{\pi}{2} \;=\; \prod_{n=1}^{\infty} \frac{2n\cdot 2n}{(2n-1)(2n+1)}.$$

It is not uncommon to prove an identity such as this by showing both sides are equal to the same quantity. Prove Wallis's formula by looking at the limit of the t-distribution as $\nu \to \infty$ and using that a probability distribution must integrate to one, and by integrating the limiting distribution using brute force as well as the functional form of the gamma function, $\Gamma(x+1) = x\Gamma(x)$.

As the above problem is far afield from the standard uses of the t-distribution, it is worthwhile to briefly remark on its inclusion in our list. First, a proof of the above result (see [3]) can introduce you to several important ideas in probability, especially the power of normalization constants (if we have a probability distribution

it must integrate to 1; this remarkably simple observation is used numerous times in mathematics to attack difficult integrals). Second, this is a wonderful example of how mathematics developed in one area can find uses in others, and illustrates the value of being well read; frequently many problems that appear intractable only look that way until a new perspective is found, and different techniques brought to the problem.

REFERENCES

[1] J. F. Box, "Guinness, Gosset, Fisher, and Small Samples," Statistical Science **2** (1987), no. 1, 45–52. http://projecteuclid.org/euclid.ss/1177013437.
[2] H. Hotelling, "British Statistics and Statisticians Today," Journal of the American Statistical Association **25** (1930) 186–190.
[3] S. J. Miller, "A probabilistic proof of Wallis' formula for π", Amer. Math. Monthly **115** (2008), no. 8, 740–745. Expanded version: http://arxiv.org/pdf/0709.2181.
[4] A. Student, "The probable error of a mean", Biometrika **6** (1908), no. 1, 1–25. http://www.aliquote.org/cours/2012_biomed/biblio/Student1908.pdf.

2012

National Museum of Mathematics

On December 15, 2012, The National Museum of Mathematics (MoMath) opened in New York City. From their homepage:

> *The National Museum of Mathematics began in response to the closing of a small museum of mathematics on Long Island, the Goudreau Museum. A group of interested parties (the "Working Group") met in August 2008 to explore the creation of a new museum of mathematics – one that would go well beyond the Goudreau in both its scope and methodology. The group quickly discovered that there was no museum of mathematics in the United States, and yet there was incredible demand for hands-on math programming.*

While there have been numerous exhibits on the connections between math and art, or wings in science museums devoted to mathematics, MoMath is entirely devoted to mathematics. Their mission?

> *Mathematics illuminates the patterns that abound in our world. The National Museum of Mathematics strives to enhance public understanding and perception of mathematics. Its dynamic exhibits and programs stimulate inquiry, spark curiosity, and reveal the wonders of mathematics. The Museum's activities lead a broad and diverse audience to understand the evolving, creative, human, and aesthetic nature of mathematics.*

Centennial Problem 2012. *Proposed by Steven J. Miller, Williams College.*

There are a lot of beautiful exhibits at MoMath. One of my favorites is riding a bike with square wheels (see Figure 3)! It's possible to do this with a catenary curve, a very famous curve in the history of mathematics (it's the same shape that a rope takes when hanging from two points – it's wonderful seeing the same results in different areas).

Just a few feet away is another interesting mode of transport. The irregularly shaped objects in Figure 4 share a property with spheres: no matter how they are lying, they are always at the same height! While it isn't surprising that one could

FIG. 3. *Glen Whitney, Co-Executive Director of MoMath, riding on a bike with square wheels on a catenary. Image from video clip at* http://www.mathaware.org/mam/2014/calendar/momath.html.

roll smoothly over a set of spheres, the fact that there are infinitely other candidates is unexpected to many (another fun fact: the sled has constant width, and can spin freely as it rolls).

FIG. 4. *Cindy Lawrence, Co-Executive Director of MoMath, demonstrating a sled of constant width which glides smoothly over shapes of constant height. Image from video clip at* http://www.mathaware.org/mam/2014/calendar/momath.html.

Find some shapes of constant height, so that no matter how they lie the distance of their highest point off the ground is constant. Can you find such shapes in all dimensions? Is there a trivial way to extend a shape that works in $d-1$ dimensions to d dimensions? If so, can you find non-trivial examples for all dimensions?

REFERENCES

[1] C. G. GRAY, "Solids of Constant Breadth", The Mathematical Gazette **56** (1972), no. 398, 289–292.
[2] L. HALL and S. WAGON, "Roads and Wheels", Mathematics Magazine **65** (1992), 283–301.
[3] MOMATH, "Museum of Mathematics homepage", http://momath.org/.

[4] R. L. Tennison, "Smooth Curves of Constant Width", The Mathematical Gazette **60** (1976), no. 414, 270–272.